This product herewith complies with requirements of EMC directive 2014/30/EU. In addition it complies with RoHS directive EN50581:2012

Northern Office
Videx Security Ltd
Unit 4-7 Chillingham ind Est
Newcastle Upon Tyne
NE6 2XX
Tel: 0870 300 1240
Fax: 0191 224 5678

Southern Office
1 Osprey
Trinity Park
Trinity Way
London
E4 8TD
Fax: 0208 523 5825

DINBIOC3 Biometric Reader

User's Manual

Contents

1. DESCRIPTION 3
2. SPECIFICATIONS 3
3. MOUNTING 3
4. WIRING 4
4.1 CONNECTING DINBIOC3 WITH DINMTPX PROXIMITY READER 4
4.2 CONNECTING DINBIOC3 WITH DINPAD-M KEYPAD 4
5. CONNECTING BIOMETRIC READERS TO EWS CONTROLLER 5
5.1 CONNECTING BIOMETRIC READERS IN SAME RS485 LINE WITH THE EWS CONTROLLERS 5
5.2 CONNECTING BIOMETRIC READERS WHEN ALL THE CONTROLLERS HAVE TCP/IP COMMUNICATION 6
6. CONNECTING BIOMETRIC READERS TO 3RD PARTY CONTROLLER 6
6.1 CONVERTERS PIN DESCRIPTION 6
7. ENROLLMENT 7
8. CONFIGURING THE BIOMETRIC READERS IN PROS SOFTWARE 7
8.1 ADDING BIOMETRIC READER 7
8.2 ENROLLING FINGERPRINTS FROM A READER 8
8.3 ENROLLING FINGERPRINTS FROM DESKTOP READER 9
8.4 DELETING FINGERPRINTS 10
8.5 UPLOADING THE FINGERPRINTS TO THE BIOMETRIC READERS 10
8.6 FIRMWARE UPDATE 11
8.7 SENSOR CALIBRATION 11
8.7 SEND CONFIGURATION 11
8.9 ADVANCED SETTING 11
9. CONFIGURING THE BIOMETRIC READERS IN BIOMANAGER 12
9.1 ADD READER 12
9.2 EDIT READER 13
9.3 DELETE READER 14
9.4 CALIBRATE SENSOR 14
9.5 ADD USER 14
9.6 EDIT USER 14
9.7 DELETE USERS 15
9.8 ENROLL FINGERS 15
9.9 UPLOAD FINGERPRINTS TO READER 15
9.10 DELETE FINGERPRINTS 16
9.10.1 Deleting one user from the biometric reader 16
9.10.2 Deleting all users from the biometric reader 16
9.11 COMPLEX USER UPLOAD 16
9.12 CUSTOM WIEGAND 17
10. WIEGAND PROTOCOL DESCRIPTION 18
11. SAFETY PRECAUTIONS 19
12. TROUBLESHOOTING 19

11. SAFETY PRECAUTIONS

Do not install the device in a place subject to direct sun light without protective cover.
Do not install the device and cabling close to a source of strong electro-magnetic fields like radio-transmitting antenna.
Do not place the device near or above heating equipments.
If cleaning, do not spray or splash water or other cleaning liquids but wipe it out with smooth cloth or towel.
Do not let children touch the device without supervision.
Note that if the sensor is cleaned by detergent, benzene or thinner, the surface will be damaged and the fingerprint can't be entered.

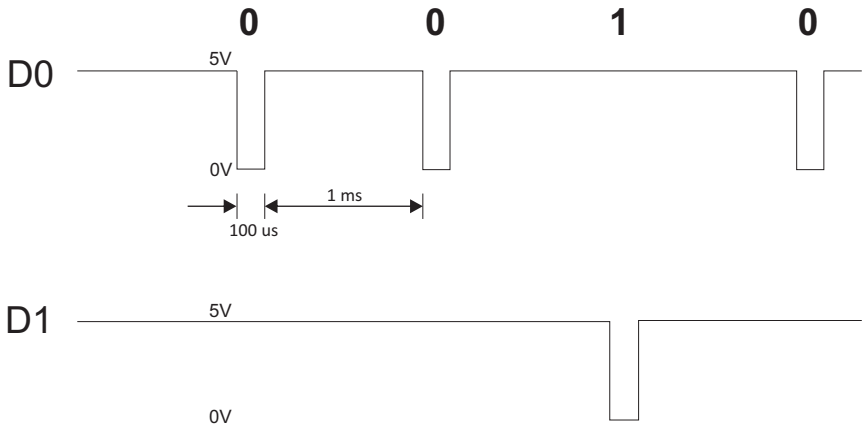
12. TROUBLESHOOTING

The Red Led on the Biometric Reader is blinking all the time	There were 15 unsuccessful attempts of authentication (Finger or PIN). The Red LED will turn off after the first accepted finger or PIN.
Enrollment from desktop reader can be done, but the Fingerprints are not sent to all Biometric Readers in the network	·Check the Ser.No of the Readers. ·Check if proper termination is done as described before Check if the Communication wires (A & B) are properly connected to the reader
The Biometric Reader is not powered ON. The tricolour LED is OFF.	Check the power Supply (red & black wire)
Fingerprint (or PIN Code) is recognized (the tricolor LED is green), but the controller reports other ID number and the access is denied	·If the user is not deleted from the reader and the same user is enrolled again with new ID, the reader will recognize the finger with the first ID. To resolve this, delete all users from the reader and upload all users to the reader ·Check the Wiegand Bus (yellow & white wire) ·Check if the ground of the controller and the Biometric Reader is the same Check if the length between Biometric Reader and the controller is less than 50 m
Electro static discharge influences the Fingerprint Scan.	Connect the housing of the Biometric Reader to the earth wire
Reader reading performance is decreased	·**Check if fingerprint reading area is dirty. Do not clean the device with any form of liquid. Use soft and dry cloth only** Reading area is damaged. If the damage is minor, try to calibrate the sensor
Fingerprint is not recognized normally	·Retry after drying the wetness of your finger ·When your finger is too dry, touch your forehead and try again When you have a cut on your registered finger, register another fingerprint

10. WIEGAND PROTOCOL DESCRIPTION

The data is sent over the lines DATA 0 for the logic “0” and DATA 1 for the logic “1”. Both lines use inverted logic, meaning that a pulse low on DATA 0 indicates a “0” and a pulse low on DATA 1 indicates a “1”. When the lines are high, no data is being sent. Only 1 of the 2 lines (DATA 0 / DATA 1) can pulse at the same time.

Example: data 0010....



Data bit 0 = approximately 100 us (microseconds)

Data bit 1 = approximately 100 us (microseconds)

Time between two data bits: approximately 1 ms (millisecond). Both data lines (D0 and D1) are high.

Description for the 26 bits Wiegand format

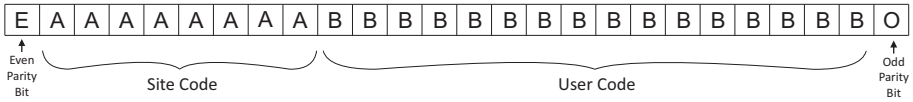
Each data block consists of a first parity bit P1, a fixed 8 bits header, 16 bits of user code and a 2nd parity bit P2. Such a data block is shown bellow:

Parity bit (bit 1)	+	8 bits header	+	16 bits user code = 2 bytes	+	Parity bit (bit 26)
P1		XXXXXXXX		XXXXYYYY YYYYYYYY		P2
Example:		170		31527		
1		10101010		01111011 00100111		0

Note: Parity bits are calculated as follows:

P1 = even parity calculated over the bits 2 to 13 (X)

P2 = odd parity calculated over the bits 14 to 25 (Y)



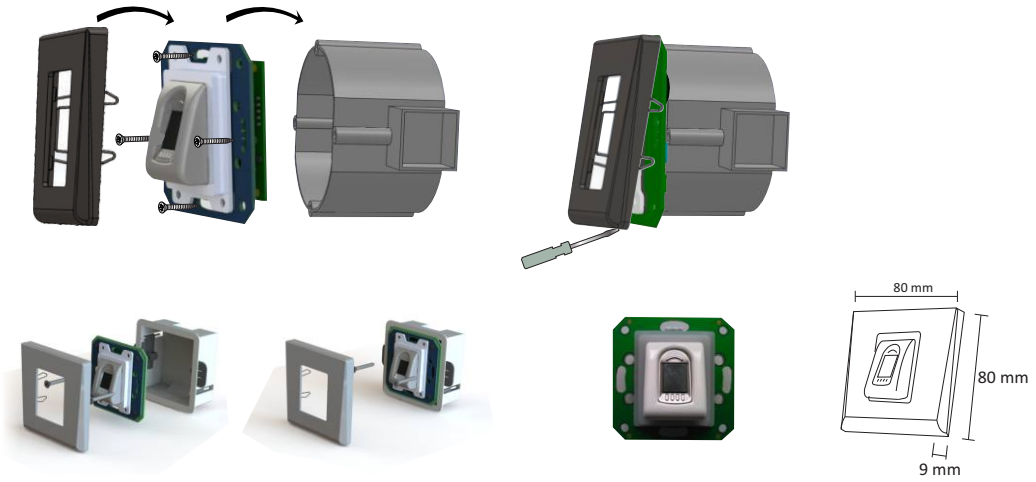
1. DESCRIPTION

DINDINBIOC3 is a Wiegand biometric reader for indoors access control applications. It offers storage up to 9500 fingerprints and programmable Wiegand Output (8 to 128 bits).
Configuration of the readers and fingerprint enrollment is done through PC Software.
Connection between the biometric readers is RS485 and it is used for fingerprint transfer and configuration.
When used with third party controllers, the connection between the Biometric readers and the PC is done through a converter (CNV100-RS485 to RS232 or CNV200-RS485 to USB or CNV300-RS485 to TCP/IP). Only one converter is needed per system (one converter for 1, 2, 3...30, 31 Biometric readers)
The tamper switch output can trigger the alarm system, if an attempt is made to open or remove the unit from the wall.

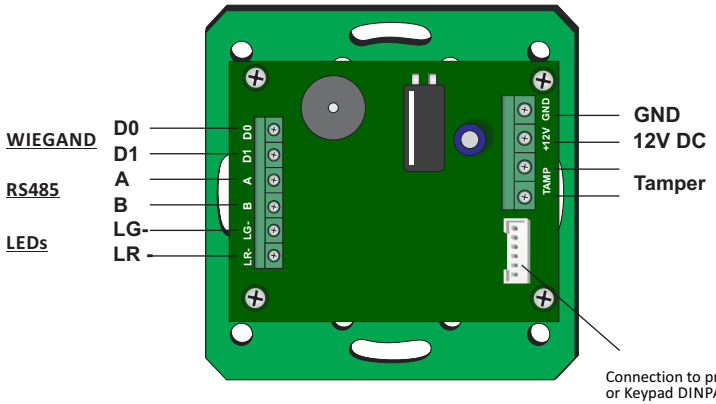
2. SPECIFICATIONS

Fingerprint capacity	up to 9500 fingerprints
Technology	Biometry
Authentication	Finger
Fingerprints per user	1-10 fingerprints
Interface	Wiegand 8 to 128 bits; Default: Wiegand 26bit
Protocol programming	By PROS CS software (EWS system) and BIOMANAGER (all access control systems)
Cable distance	50m
Fingerprint Sensor Type	Capacitive
1:1000 identification time	970 msec, including feature extraction time
Fingerprint enrolment	On the reader or from the USB desktop reader (BIOE)
Panel Connection	Terminal blocks
Green and Red LED	Externally Controlled
Orange LED	Idle mode
Buzzer	Yes
Backlight ON/OFF	Yes, by software settings
Tamper	Yes
Consumption	100mA
IP Rating	40
Power supply	9-14V DC
Operating Temperature	0°C to +40°C
Dimensions (mm)	80 x 80 x 36
Frame Colour	Silver, Red, Green, Dark Grey, Blue, White

3. MOUNTING



4. WIRING



12V DC	9-14V DC
GND	ground
A	RS485 A
B	RS485 B
LR-	Red LED -
LG-	Green LED -
D1	Data 1
D0	Data 0
Tamper	Tamper Switch(NO)
Tamper	Tamper Switch(NO)

4.1 CONNECTING DINBIOC3 WITH DINMTPX PROXIMITY READER

1. Connect both devices with the cable provided. (fig. 1)
2. Connect theDINBIOC3 to the controller. The proximity reader is not connected to the controller. (fig. 2)
3. In the software, in reader's properties, for type of the reader select DINBIOC3+DINMTPX. (fig. 3)

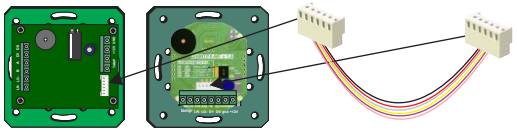


fig. 1

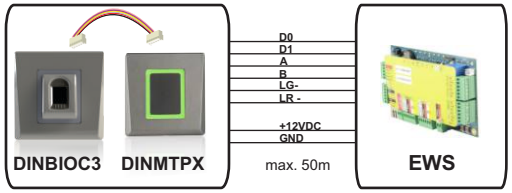


fig. 2

fig. 3

4.2 CONNECTING DINBIOC3 WITH DINPAD-M KEYPAD

1. Connect both devices with the cable provided. (fig. 1)
2. Connect the DINBIOC3 to the controller. The Keypad is not connected to the controller. (fig. 2)
3. In the software, in reader's properties, for type of the reader select DINBIOC3+DINPAD-M. (fig. 3)
4. Put the Keypad to work as **Slave** unit. (fig. 4)

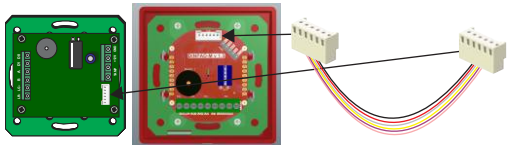


fig. 1

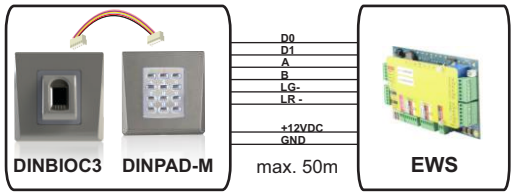


fig. 2

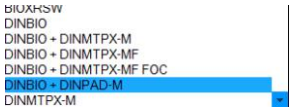
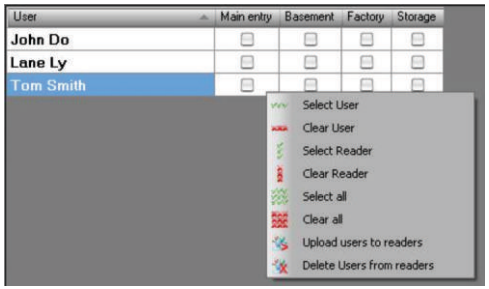


fig. 3

Press B+000000
Press 0
Press 2
Press A to exit

fig. 4

Use mouse click to select the combination you need or use right-click to check or clear entire row or column

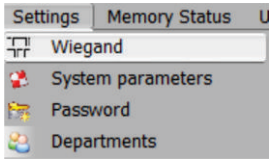


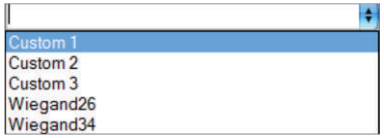
Select **Upload Users to readers** or **Delete Users from readers** at right-click menu
As upload is progressing, check boxes are cleared mining appropriate combination was successfully done
When upload is over, if there are still checked items, repeat the upload command

9.12 CUSTOM WIEGAND

BioManager has defined Wiegand 26 and 34 bit as standard options and other 3 Wiegand settings as user definable.

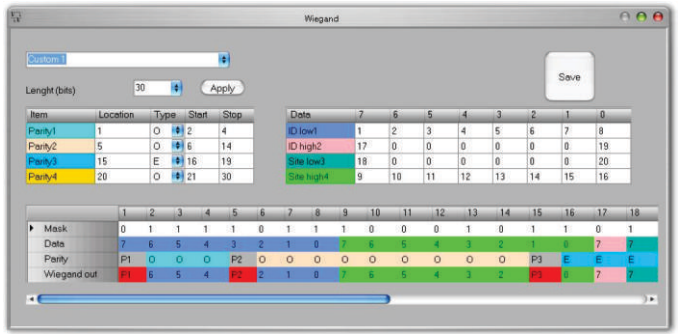
To setup custom Wiegand format
Select **Wiegand** menu from **Settings**





At Wiegand setup window select one from customs Wiegand

Set Wiegand parameter



Click on **Save** button

Note:
Wiegand settings are out of scope for common end user. Please ask your installer to set the parameters and do not change it later.

For more information please refer to BioManager User Manual

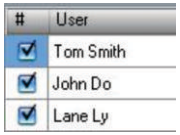
9.10 DELETE FINGERPRINTS

After the transfer, the fingerprint are stored in the Biometric reader and in the PC.

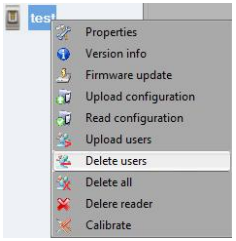
Deleting can be done only in the software, only in the readers or from the both places.

9.10.1 Deleting one user from the biometric reader

Select the users checkbox.

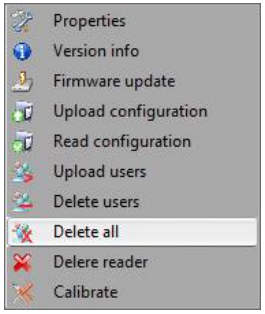


Right click on the Reader and select **Delete Users**



9.10.2 Deleting all users from the biometric reader

Right click on the Reader and select **Delete all**



The user is deleted from the reader, but his fingerprints are still in the software's database. They can be sent ones again without the need of re enrollment.

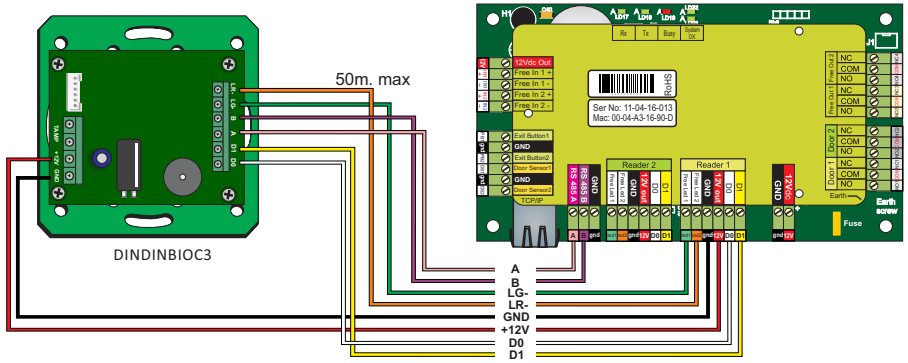
9.11 COMPLEX USER UPLOAD

Complex user upload is used to sent multiply user selection to more readers

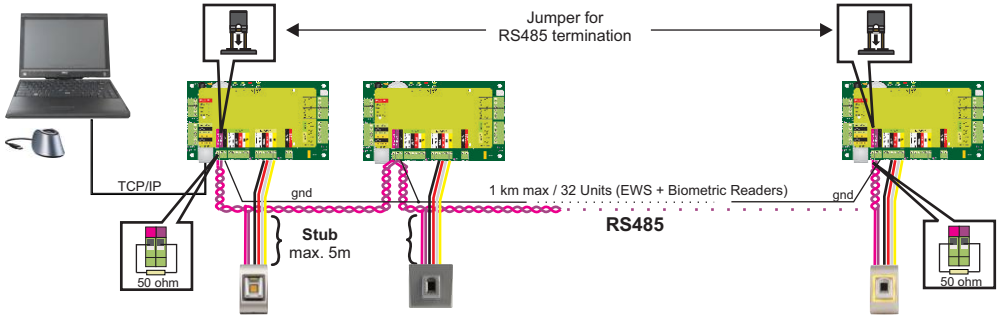
Click on **Upload table** at main menu

5. CONNECTING BIOMETRIC READERS TO EWS CONTROLLER

- The Biometric readers can be connected to virtually any controller that conforms to Wiegand format standards (standard Wiegand 26bit or self-defined Wiegand).
- The lines D0 and D1 are the Wiegand lines and the Wiegand Number is sent through them.
- The RS485 line (A, B) is used for fingerprint transfer and reader settings.
- The Biometric readers must be powered from the controller.
- If you use different power supply for the biometric reader, connect the GND from the both devices to ensure correct transfer of the wiegand signal
- When you have connected the reader and powered on, the LED should flash in orange light + 2 beeps. This lets you know it's on and ready for use.
- Fingerprint enrollment is done from the PC Software. Connection between the Biometric readers and the PC must be established.

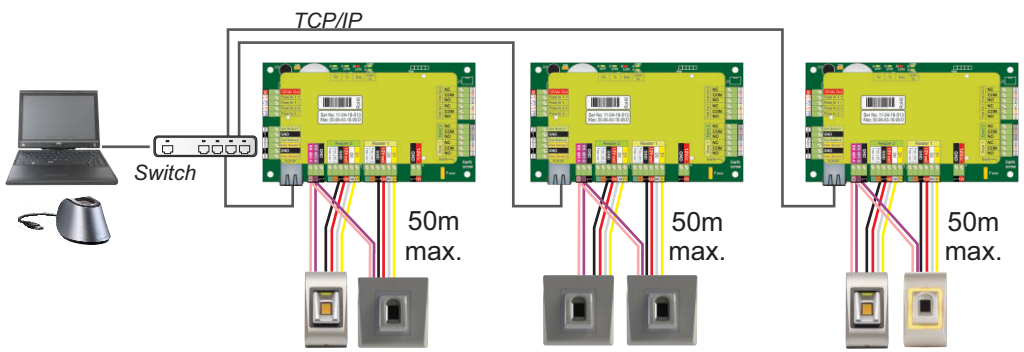


5.1 CONNECTING BIOMETRIC READERS IN SAME RS485 LINE WITH THE EWS CONTROLLERS



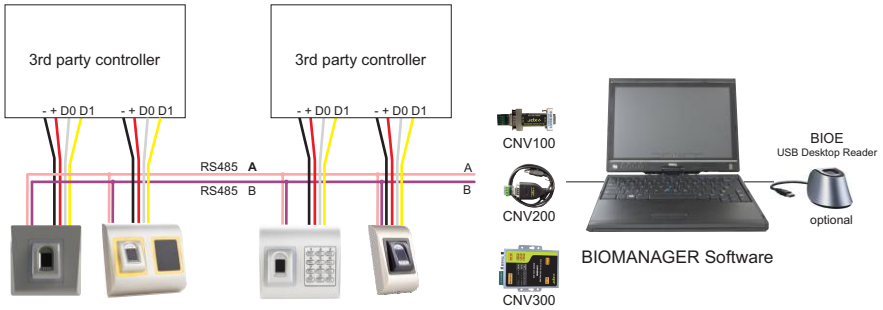
- The Biometric readers are connected through RS485 bus. The same RS485 bus that the EWS controllers are connected to.
- Maximum units in one network (EWS + Biometric readers) is 32.
- If there are more than 32 units in one network, please utilize RS 485 HUB to connect.
- The RS485 Line should be configured in the form of a daisy chain, NOT in a form of a star. If star must be used in some points, keep the stubs from the RS485 backbone as short as possible. Maximum length of the stub is dependant of the installation (total number of devices in RS485 line (total cable length, termination, cable type...) so recommendation is to keep stubs shorter than 5 meters, keeping in mind that this can be possible reason for errors in communication with PC software
- The cable must be twisted and shielded with a min. 0.2 mm2 cross section.
- Connect the ground (0V) of each unit in the RS 485 Line using a third wire in the same cable.
- The shield of the communication cable between two devices must be connected to the EARTH from ONE side of the RS 485 Line. Use the side that has earth connection to the building's grounding network.

5.2 CONNECTING BIOMETRIC READERS WHEN ALL THE CONTROLLERS HAVE TCP/IP COMMUNICATION



- When all the controllers are connected via TCP/IP, then the RS485 network becomes local (from Reader 1 to the Controller then to the Reader 2).
- Connect the readers directly to the Rs485 terminals in each controller.
- If the distance Reader-Controller is high (50meters) and if the communication with the reader can not be established, then terminate the RS485 network by closing the jumper in the EWS Controller or as described in chapter 4.

6. CONNECTING BIOMETRIC READERS TO THIRD PARTY CONTROLLERS



- Connect the lines D0, D1, Gnd and +12V to the third party controller.
- Connect the RS485 Line (A, B) to the converter. Connect the converter in the PC.
- Fingerprint enrollment is done from the PC Software. Connection between the Biometric readers and the PC must be established.
- The Biometric readers communicate with each other with a RS485 and with the PC Software through a Converter.
- The RS485 Line should be configured in the form of a daisy chain, NOT in a form of a star. Keep the stubs from the RS485 backbone as short as possible (not more than 5 meters)
- Only one converter per installation is needed, not per reader.

6.1 CONVERTERS PIN DESCRIPTION

CNV100
Converter RS485 to RS232
Does not requires installation

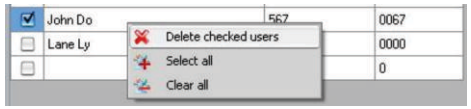
Biometric Reader	Converter
RS 485 A	PIN 1 (RS 485 +)
RS 485 B	PIN 2 (RS 485 -)

CNV200
Converter RS485 to USB
Requires installation as USB serial device (refer to CNV200 Manual).
The Drivers are located on the CD.

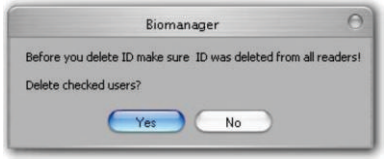
CNV300
Converter RS485 to TCP/IP
Does not require installation. IP address set through Internet Browser(refer to CNV300 Manual)

9.7 DELETE USERS

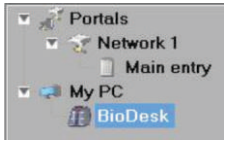
- Check the users to be deleted
- Right-click on the users table
- Click on **Delete checked users menu**



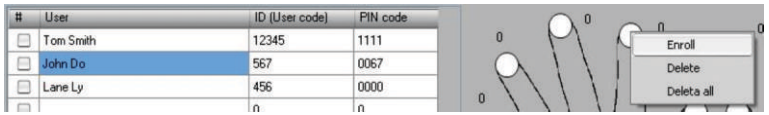
Confirm warning message



9.8 ENROLL FINGERS



- Select the User in the User Column, not the check box (the check box is for sending the fingerprints) and the User name cell will turn blue
- Select the Biometric reader or Desktop reader BIOE from where the enrollment will be done



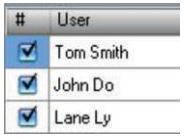
Right click on the fingertip and select **Enroll**

Swipe the finger on the Reader and the finger tip will become blue, with percentage of successful enrollment given right beside the fingertip

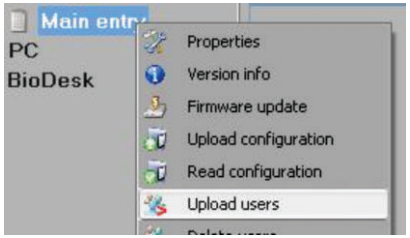
Note: If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller.

9.9 UPLOAD FINGERPRINTS TO READER

Check the users which fingerprints will be sent to the Reader



Right-click on the Biometric reader those users should be sent and select **Upload users**

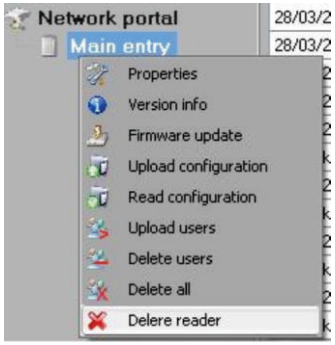


As each user is being sent, the checkbox will become unchecked indicating that the user is successfully sent. In the same time the orange LED of the Biometric reader blinks

Note: Average time for transferring one finger template is 0,6 sec.
Note: The PIN Codes are also being sent, if there are any.

9.3 DELETE READER

Right-click on the reader and select **Delete reader**



9.4 CALIBRATE SENSOR

Right-click on the reader and select **Calibrate**

See the events panel to check the calibration flow

It is recommended to do sensor calibration once after reader is mounted. Clean the fingerprint sensor before calibration.

9.5 ADD USER

At user table, click on the last empty user field and enter user name

#	User	ID (User code)	PIN code
	Tom Smith	12345	1111
		0	0

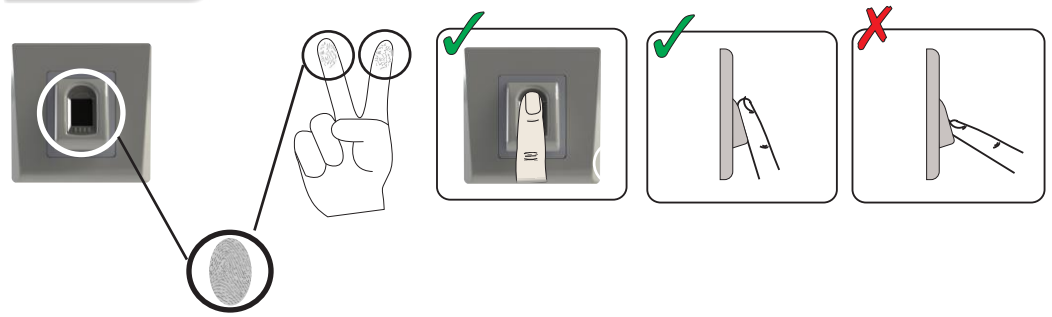
Click on ID (User code) field and enter ID number. This number will be sent by the reader to the access controller when user finger is recognized by the reader
Click on PIN code field and enter the PIN. PIN code is used at readers with keypad. When PIN code is typed at reader, User ID will be sent to the access controller

9.6 EDIT USER

- Find the user at user table to edit
- Click on the user field for edit (Name, ID or PIN)
- Type new value
- Press Enter on the keyboard

Important:
When ID is changed, warning message is displayed reminding that if ID exist in some reader, should be deleted from reader prior to change.

7. ENROLLMENT

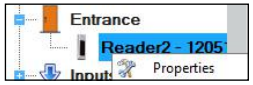


8. CONFIGURING THE BIOMETRIC READERS IN PROS CS SOFTWARE

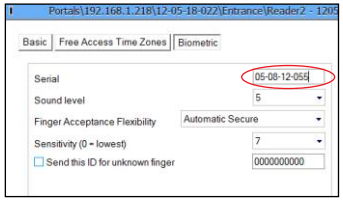
8.1 ADDING BIOMETRIC READER

1. Expand the Door item to view the readers
2. Right click on the reader and select properties (8.1)
3. In the Basic tab, for “Type” of the Reader select “DINBIOC3”. (8.2)
4. After selecting the type, a third tab will appear “Biometric”. Go to that tab and put the serial number of the Biometric Reader. (8.3)

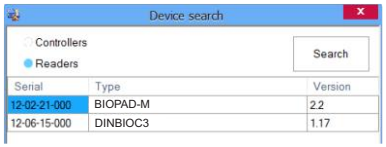
Important Note: The serial number of the reader can be found on a sticker inside the reader, on the packaging box and it can be search from the software (right click on the portal/search devices/readers). (8.4 & 8.5)
To check if the reader is On Line, right click on the reader and select “Check version”. In the Event Window a message should appear “Device ON Line, Type: DINBIOC3” (8.6)



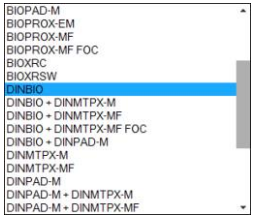
8.1



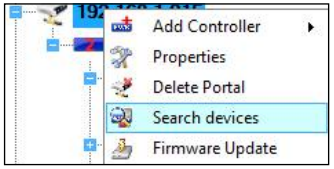
8.3



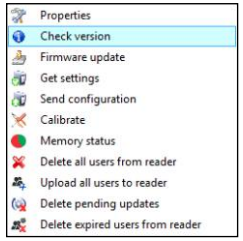
8.5



8.2



8.4



8.6

8.2 ENROLLING FINGERPRINTS FROM A READER

1. Open the Users Window and create a new user.
   Click on “New User”, put a name and ID(card number). (8.7)
2. Go to the “Biometric” Tab
3. Select the reader(with left click) from which the enrollment will be done. (8.8)
4. Right click on the fingertip and select enroll. (8.9)
5. In the next 25 sec. present the finger on the selected reader and the finger tip will turn red, with the percentage of successful enrollment shown next to the fingertip. (8.10)
   In these 25 sec. the reader will continuously blink in orange.
6. Repeat point 4&5 for each finger that should be enrolled.
7. Click on “Save New” and the fingerprint will be sent automatically to all Biometric Readers where that user has access, i.e. to all the readers according to the Access Level assign to that user.

Example:

If the user has “Unlimited” Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

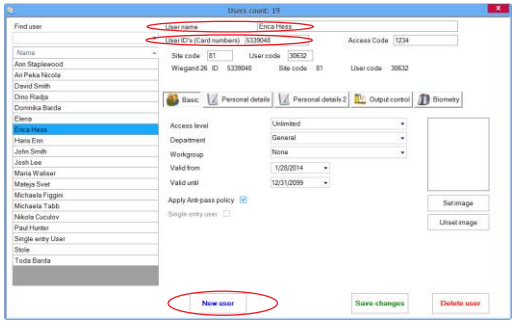
Note:

To check if all the fingerprints are sent to the reader, right click on the reader and select “Memory Status”. (8.11)

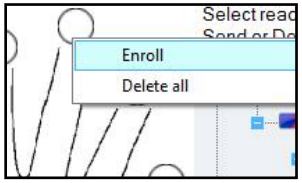
In the event window a line will appear indicating the number of fingerprints stored in the reader. (8.12)

Note:

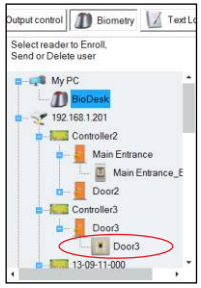
If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).



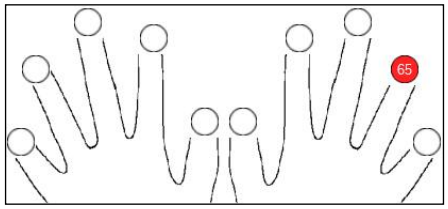
8.7



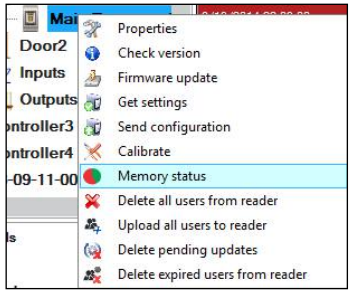
8.9



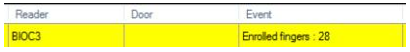
8.8



8.10



8.11

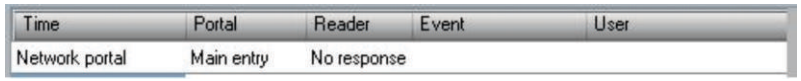


8.12

If reader is online, new line is added on top of the event table

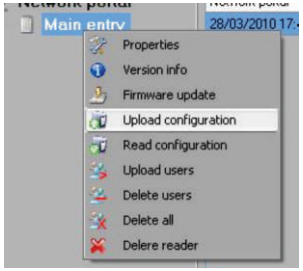
Time	Portal	Reader	Event	User
28/03/2010 17:41:30	Network portal	Main entry	Device online	Type: BioXr Version: 1.22

If reader is not online, following line is added on top of the event table

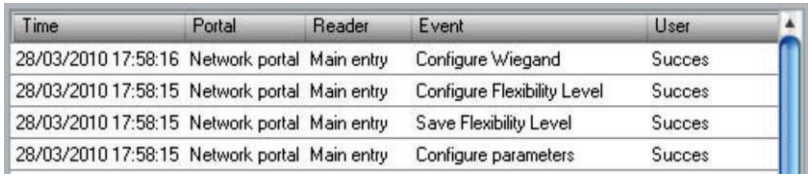


Time	Portal	Reader	Event	User
Network portal	Main entry	No response		

If reader is online, right click on reader and select **Upload configuration**



Check at event table if configuration was successful

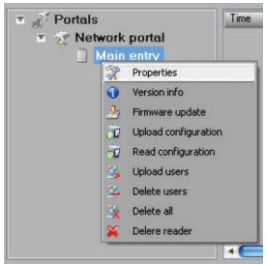


Time	Portal	Reader	Event	User
28/03/2010 17:58:16	Network portal	Main entry	Configure Wiegand	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Save Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure parameters	Succes

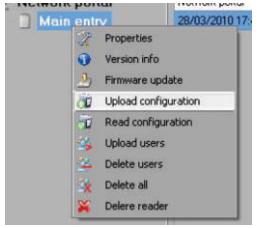
9.2 EDIT READER

Right-click on the reader and select **Properties**

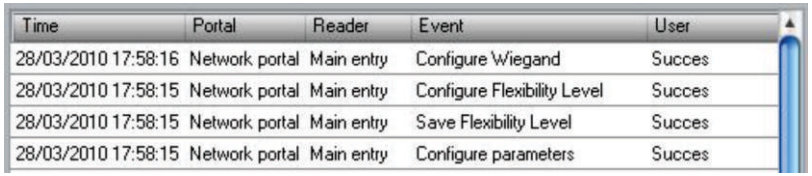
Edit reader properties and click **Save** button



Right click on the reader and select **Upload configuration**



Check at event table if configuration was successful



Time	Portal	Reader	Event	User
28/03/2010 17:58:16	Network portal	Main entry	Configure Wiegand	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Save Flexibility Level	Succes
28/03/2010 17:58:15	Network portal	Main entry	Configure parameters	Succes

9 CONFIGURING THE BIOMETRIC READERS IN BIOMANAGER

BioManager is software for fingerprint management of Videx Biometric readers, when used with third party access controllers.

Main functions:

- Fingerprint Enrollment
It can be done by ANY Biometric reader in the network or by Desktop (USB) Biometric reader.
Note: The Desktop Biometric reader BIOE is only compatible to Biometric readers with capacitive sensor, not with the ones with thermal sensor.

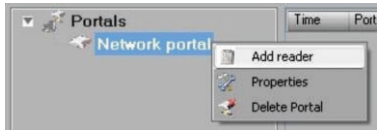
- Fingerprint Transfer
Finger templates can be sent to any Reader in the Network. Different Users can be sent to different Biometric readers.

- PIN Codes management and transfer
PIN Code length configuration (1 to 8 digits) and PIN Code transfer.

- Wiegand Output Configuration
The Wiegand output of the Biometric reader can be customized bitwise.

9.1 ADD READER

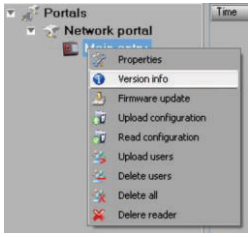
Right-click on the portal connected to the reader and select Add reader



Fill the Reader form

Click on **Save** and the reader icon appears under the selected portal

Right-click on reader and select **Version info**



8.3 ENROLLING FINGERPRINTS FROM DESKTOP READER

Plug the Desktop Reader (BIOE) in the PC. If the device is not installed automatically use the drivers located on the CD provided with the Biometric reader. It is installed in the same way as a USB Device. When the desktop reader has been installed it will automatically appear in the Software. (8.13)

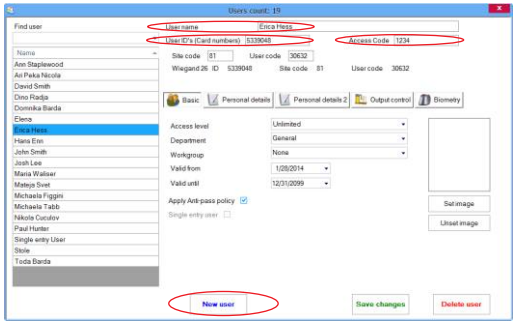
1. Open the Users Window and create a new user.
   Click on "New User", put a name and ID(card number). (8.7)
2. Go to the "Biometric" Tab
3. Select the USB desktop Reader (with left click).
4. Place the finger on the BIOE, right click on the fingertip and select enroll. (8.9)
5. The finger tip will turn red, with the percentage of successful enrollment shown next to the fingertip. (8.10)
6. Repeat point 5 for each finger that should be enrolled.
7. Click on "Save New" and the fingerprint will be sent automatically to all Biometric Readers where that user has access, i.e. to all the readers according to the Access Level assign to that user.

If the reader is off line, the fingers will be sent upon the connection is established between PROS server and the reader. No need for additional enrollment or actions. The fingerprints will be sent as soon as communication is established.

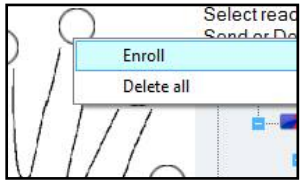
Example:
If the user has "Unlimited" Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

Note:
To check if all the fingerprints are sent to the reader, right click on the reader and select "Memory Status". (8.11)
In the event window a line will appear indicating the number of fingerprints stored in the reader. (8.12)

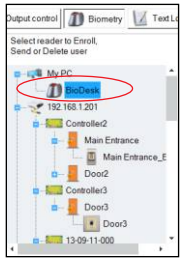
Note:
If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).



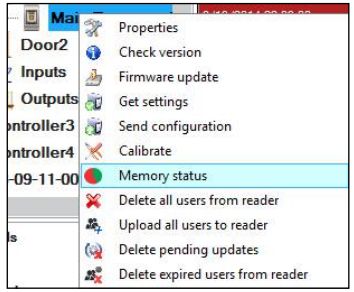
8.7



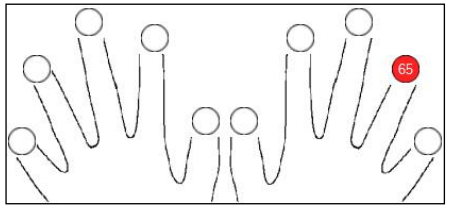
8.9



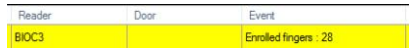
8.13



8.11



8.10



8.12

8.4 DELETING FINGERPRINTS

In General, the fingerprints are stored in the Biometric reader and in the Software.
Deleting can be done only in the readers or from both places.

Deleting one user from the biometric reader

Select the User
Click on “Delete User”. The User together with its fingerprints will be deleted from both the software and the fingerprint readers. (8.14)

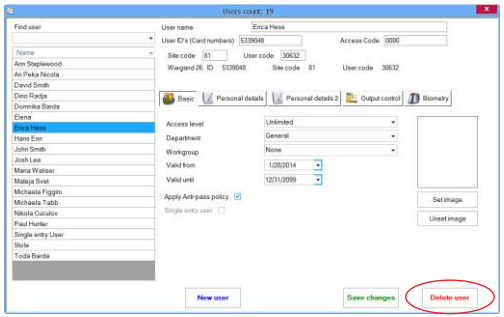
Deleting all users from the biometric reader

Right click on the reader and select “Delete all users from reader” (8.15)

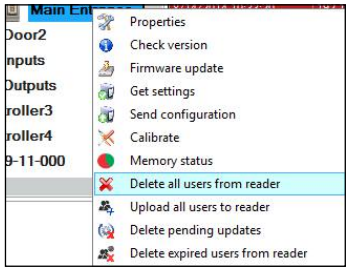
Delete one or more fingerprints

Select the User and open the “Biometric” tab
Go to the fingertip that needs to be deleted, right click and select ”Delete” for one finger or “Delete All” for all fingers of the User.
Click “Save Changes”.

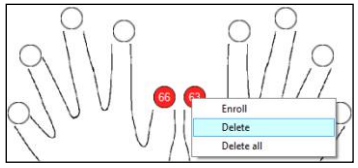
With this procedure the User's fingerprints are deleted from the software and from the reader. (8.16)



8.14



8.15

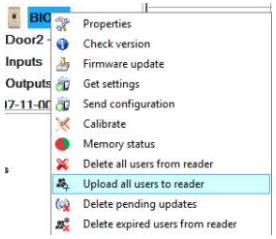


8.16

8.5 UPLOADING THE FINGERPRINTS TO THE BIOMETRIC READERS

Right click on the biometric reader
Select “Upload all users to reader”
While receiving the fingerprints the reader will blink in orange.

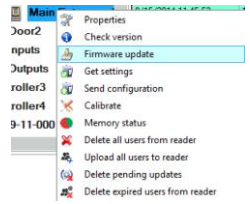
Note: Use this feature when you change or add a reader, if pending tasks are deleted in the software or if there are doubts that fingerprints in the reader memory are not synchronized with the software database.
In normal usage, the fingerprints are sent automatically and this feature is not used.



8.17

8.6 FIRMWARE UPDATE

Right-click on the reader and select Firmware update menu (8.18)
On the Firmware update window, click on the Browse button (8.19). The default location of the firmware files installed with PROS CS is in the folder "Firmware".
Select the firmware file with a "xhc" extension.
Click on the Upload button
Important: Wait for the update end message. Do not turn off the reader, the software or any communication device in between during the entire process.



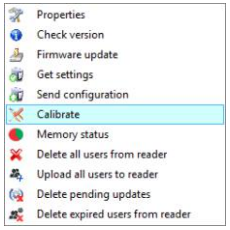
8.18

8.19

8.7 SENSOR CALIBRATION

Right click on the biometric reader and select “Calibrate” and wait for confirmation message.

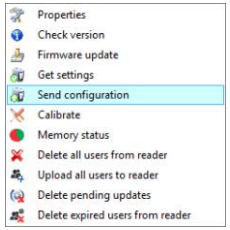
Note: It is recommended to do a calibration while commissioning the reader and in cases when there are problems with reading the fingers



8.8 SEND CONFIGURATION

· Right-click on the reader and select the Send configuration menu
· See the events panel to check the configuration flow

Note: The biometric reader gets its settings automatically. This function is used if the reader was off line while making the changes.



8.9 ADVANCED SETTINGS

Send This ID for:
Unknown Finger sends the desired Wiegand when an unknown finger is applied.

Click on the Save & Exit button

Backlight:
Backlight of the device (ON or OFF)
Finger Acceptance Flexibility:
Accepted tolerance. The recommended value is “Automatic Secure”.
Sensitivity:
Bio-sensor sensitivity, the recommended value is 7, most sensitive.